<https://www.toz.khv.ru/newspaper/obratite_vnimanie/kak_zashchitit_svoyu_plastikovuyu_kartochku_ot_moshennikov/>

[](https://www.toz.khv.ru/)

**Как защитить свою пластиковую карточку от мошенников**

**19.01.2017** **|** [**Обратите внимание**](https://www.toz.khv.ru/newspaper/obratite_vnimanie/)

Операции с использованием банковских карт уже давно стали не­отъемлемой частью нашей повседневной жизни. Карты упрощают процесс оплаты товаров и услуг, а также помогают защитить денежные средства, ведь украденная карта бесполезна, если не знать её ПИН-код, в отличии, например, от кошелька с наличными деньгами.

- Но безопасность средств, хранимых на банковском счете, зависит в первую очередь от соблюдения держателем карты правил её использования: небрежное обращение с картой работает на руку мошенникам, которые постоянно изыскивают новые способы обмана, - предупреждает Наталья Прокаева, ведущий экономист краевого отделения ДГУ Центрального банка РФ.

**Две стороны прогресса**

- Для удобства клиентов банки предлагают услугу дистанционного управления своими счетами с компьютера или мобильного телефона через специальные онлайн-приложения, - говорит Наталья Прокаева. - На сегодняшний день практически у каждого человека есть универсальный гаджет, помогающий оплачивать покупки или услуги. Используя такие устройства, клиенты банков получают банковские услуги буквально не выходя из дома в режиме реального времени. При этом сервисы, предлагаемые банками для обслуживания клиентов в онлайн-среде, проходят специальную сертификацию, подтверждая свою надежность и высокую степень безопасности.

Но у технического прогресса есть и обратная сторона: вместе с развитием банковских технологий, к сожалению, совершенствуются и методы проведения мошеннических операций. Интернет-злоумышленники разрабатывают специальные вирусы и вредоносное программное обеспечение, чтобы похищать денежные средства со счетов держателей карт, подключенных к онлайн-банкингу. Они маскируют эти вирусы под безобидные приложения или рассылают их в качестве спам-сообщений.

Заражение устройства вирусами происходит, как правило, при переходе пользователя на сомнительные сайты по ссылкам, содержащимся в сообщениях (СМС, ММС или в электронной почте), либо при открытии файлов, находящихся во вложениях.

**Как происходит «заражение»**

- Пользователь получает сообщение или письмо на электронную почту, содержащее информацию интригующего или тревожного характера, например - о неожиданном выигрыше или блокировке его банковской карты, - говорит Наталья Прокаева. - Под воздействием эмоций каждый может потерять бдительность и открыть письмо, где находится файл или ссылка с предложением заполнить специальную форму. Однако делать этого ни в коем случае нельзя, так как при переходе по ссылке или при открытии файла на персональное устройство пользователя загружается вирус, который впоследствии будет перехватывать вводимые пароли и отсылать их разработчику вируса для дальнейшего взлома установленных на устройстве онлайн- и мобильных банков.

Владелец счета может даже не подозревать о списаниях, потому что в ряде случаев вирус скрывает от клиента поступающие уведомления от банка. В итоге держатель карты, не зная о несанкционированном списании с его банковского счета, не может направить в банк в определенные законодательством сроки уведомление о переводе денежных средств без его согласия. Следовательно, теряет время и право на возмещение неправомерно списанных денежных средств.

**Способы защиты**

Таким образом, безопасность денежных средств, находящихся на счетах, связана с тем, насколько ответственно пользователь относится к безопасности устройства, используемого для осуществления переводов денежных средств.

Во избежание хищения денежных средств с ваших счетов Банк России рекомендует не терять бдительности и соблюдать ряд простых правил:

- установить на ваше устройство (компьютер, ноутбук или мобильный телефон) надежное антивирусное программное обеспечение и регулярно проводить его обновление - это поможет защитить устройство от проникновения вредоносных программ;

- на устройстве, используемом для работы с системой онлайн-банкинга, исключить посещение сайтов сомнительного содержания, загрузку и установку нелицензионного программного обеспечения;

- проверять защищенность web-сайтов. Безопасные web-сайты отмечены значком в виде закрытого замочка, в строке браузера адрес сайта должен начинаться с последовательности https://;

- не открывать сообщения и не переходить по ссылкам, приходящим из недостоверных источников;

- при обнаружении несанкционированного списания средств отключить устройство от Интернета и немедленно обратиться с соответствующим заявлением в обслуживающий банк.

- Мошеннические способы, направленные на хищение средств со счетов банковских карт, могут быть разными, - говорит Наталья Прокаева, - а способ обезопасить себя и свои деньги только один - соблюдать правила безопасного использования банковских карт.

Следователями УМВД России по городу Комсомольск-на-Амуре доказана причастность граждан, обвиняемых в хищении денежных средств путем обмана и злоупотребления доверием. Ущерб составил порядка 150 тысяч рублей.

В ходе предварительного следствия было установлено, что 29-летний ранее судимый житель Приморского края разместил на интернет-сайте объявление о помощи в выдаче водительских удостоверений. Вскоре ему позвонила 32-летняя комсомольчанка и попросила предоставить ей данную услугу. Обговорив с предпринимателем все детали сделки, заявительница перевела на его банковский счет денежные средства в сумме 52 тысячи рублей. После этого мужчина перестал выходить на связь.

Еще одной жертвой интернет-мошенника стал житель Ямало-Ненецкого автономного округа. Мужчина увидел в социальной сети объявление о продаже автозапчастей, связался с продавцом и перечислил на его счет в качестве аванса денежные средства в сумме порядка 45 тысяч рублей. Вскоре телефон продавца оказался недоступен, а товар так и не пришел к своему покупателю.

К совершению данного преступления следственными органами была доказана причастность 28-летнего комсомольчанина. На допросе мужчина признался еще в двух преступных деяниях аналогичного характера. Общий ущерб, причиненный фигурантом гражданам Российской Федерации, составил порядка 100 тысяч рублей.

Как сообщает пресс-служба УМВД России по Хабаровскому краю, в настоящее время расследования завершены. Уголовные дела, возбужденные по признакам состава преступления, предусмотренного статьей 159 Уголовного кодекса Российской Федерации «Мошенничество», с обвинительным заключением направлены в суд для дальнейшего рассмотрения по существу.

До вынесения приговоров обвиняемые будут находиться под подпиской о невыезде.

Автор: Виктор ИЛИН